DETECTING AND RESPONDING TO CYBER ATTACKS IN HEALTHCARE

Gabriel Doncel
Director Information Security
Drexel University

Gabriel Doncel MBA MS CISSP

Director Information Security
Drexel University / Drexel College of Medicine

Gabriel Doncel joined Drexel University in 2019 where is currently Director of Information Security. He is also part of the University of Delaware and Wilmington University Adjunct Faculty. As a member of the Information Security team at Drexel, and working closely with the campus community and outside parties, his focus is to protect the people, information and systems of Drexel University. Prior to joining Drexel, Gabriel was Cybersecurity Resiliency Program Manager at Christiana Care Health System. He earned a Bachelor of Science degree in Computer & Network Security from Wilmington University, a Master of Science degree in information Systems and Technology Management, and a Master in Business Administration, both from the University of Delaware.

Certifications include: CISSP, C|CISO, CEH

Drexel University

Founded in 1891 in Philadelphia

- Three Philadelphia campuses and other regional sites.
- The Academy of Natural Sciences of Drexel University, the nation's oldest major natural science museum and research organization.

Enrollment

- 25,000 total students

Academic Offerings

- Over 200 degree programs
- 15 colleges and schools

Technology Leadership

- First university to require all entering students to have microcomputers (1983)
- First major university to operate a fully wireless campus, indoors and out (2000)

Mission

Drexel University fulfills our founder's vision of preparing each new generation of students for productive professional and civic lives while also focusing our collective expertise on solving society's greatest problems. Drexel is an academically comprehensive and globally engaged urban research university, dedicated to advancing knowledge and society and to providing every student with a valuable, rigorous, experiential, technology-infused education, enriched by the nation's premier co-operative education program.

Agenda

- We Are Under Attack!
- Visibility
- Incident Management
- Workflows and Playbooks
- Threat Intelligence
- Collaboration
- Trends
- Questions?

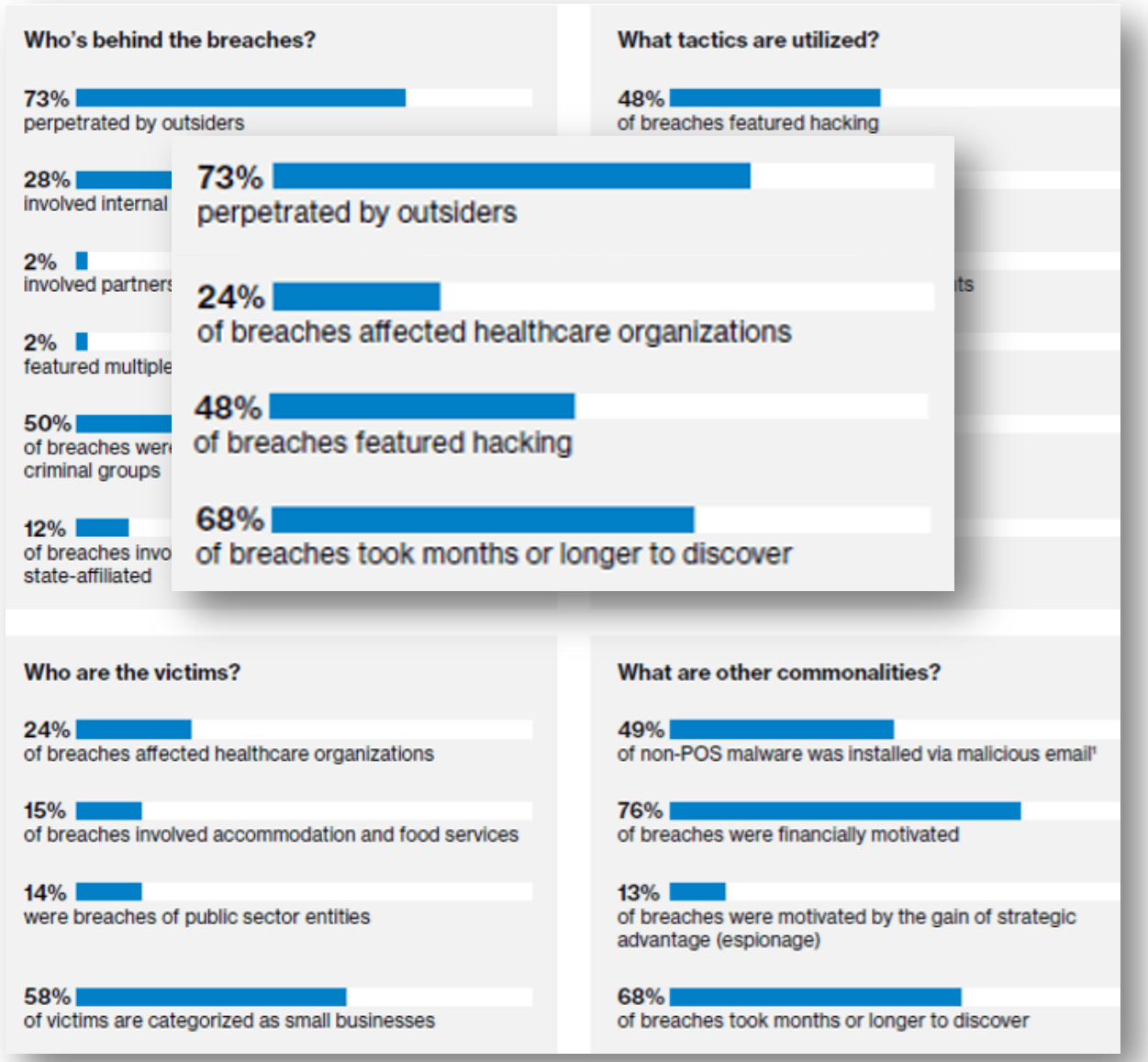
WARNING!

We're Under Attack!

MAJOR HEALTHCARE BREACHES

- Anthem Blue Cross
  78.8 Million affected
- Premera Blue Cross
  11+ Million affected
- Excellus BlueCross BlueShield
  10+ Million affected
- TRICARE
  4.9 Million affected
- UCLA Health
  4.5 Million affected
- Community Health Systems
  4.5 Million affected
- Advocate Health Care
  4+ Million affected
- Medical Informatics Engineering
  3.9 Million affected
- Banner Health
  3.62 Million affected

Verizon Data Breach Investigations Report (DBIR)



Visibility

- **Increasing number of vendors in the security space!**
  - Commercial
  - Open-source
  - In-house
- **Data Aggregation**
- **Bi-Directional integrations where appropriate**
  - Future Response Capability

2018/19 Cyber Startups

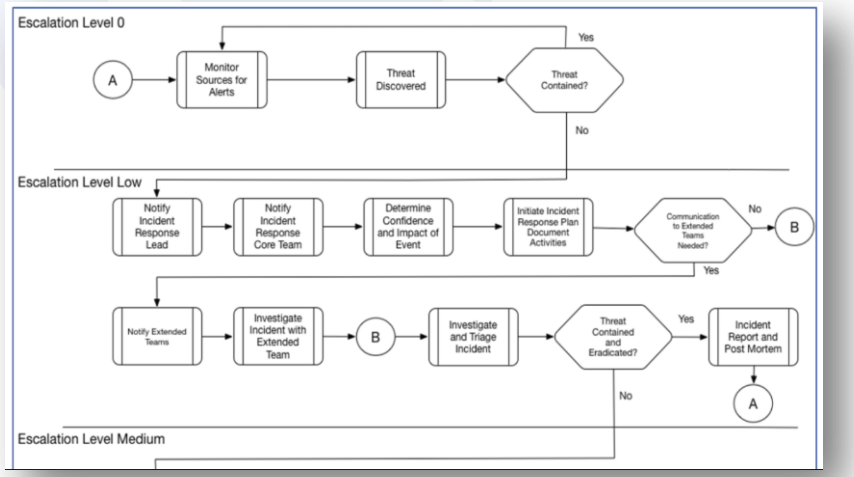
Incident Management

- Discovery / Reporting
- Response
- Investigation
- Recovery
- Follow-up

Maturity level		Ad hoc		Maturing		Strategic
Existing capabilities		As needed	Dedicated part-time	Full-time	SOC/IR+	Fusion
	People	• 0–1	• 1–3 • specialization	• 2–5 • Formal roles	• ~10 • Shifts (possible 24x7)	• 15+ • Intel, SOC, and IR teams
	Process	• Chaotic and relying on individual heroics reactive • General purpose run book • Tribal knowledge	• Situational run books; some consistency • Email-based processes	• Requirements and workflows documented as standard business process • Some improvement over time	• Process is measured via metrics • Minimal threat sharing • Shift turnover • SLAs	• Processes are constantly improved and optimized • Broad threat sharing • Hunt teams
	Technology		• SIEM • Sandboxing	• Continuous monitoring • Endpoint forensics • Tactical intelligence	• Malware analysis • Additional intelligence • IT operations	• Intel+IR drives security program • Strategic intelligence • Coordination with physical security
CMM equivalent		Initial	Repeatable	Defined	Managed	Optimized

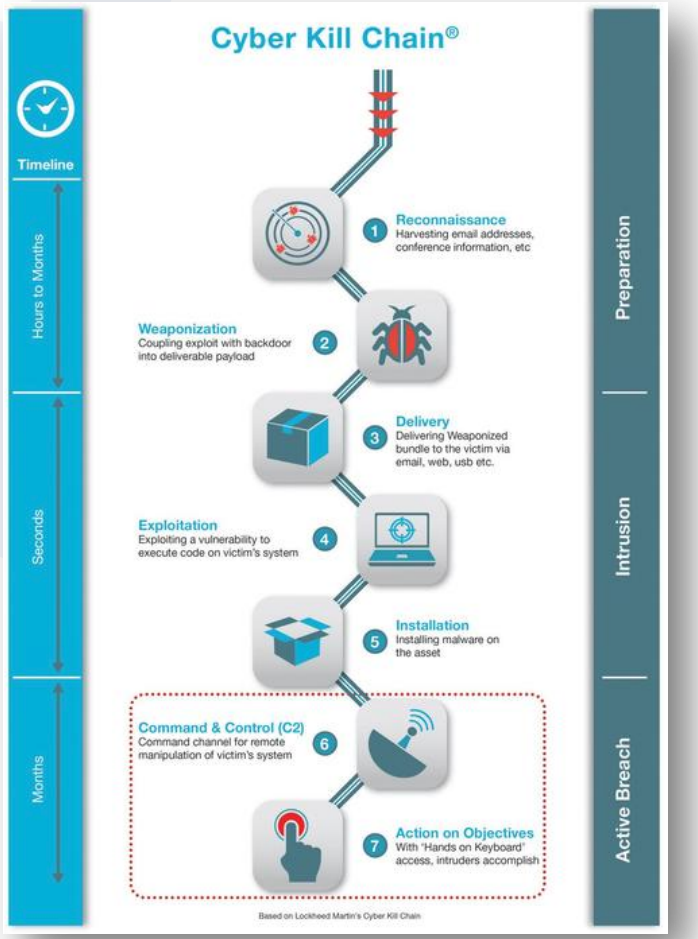
Workflows and Playbooks

- **Based on experience**
- **NIST.SP.800**
  - Brute Force
  - Web / Email
  - Loss or Theft of Equipment
  - Telecommuting Compromise
- **Utility / Facility failures**
- **Natural disasters**
- **Table-top exercises**



Threat Intelligence

- **Aggregation of indicators of compromise (IOCs)**
- **Relevant**
- **Integration into existing tools**
  - Built into the tools
  - 3rd parties
- **Visibility along the Cyber Kill Chain ®**
- **Subscription models**
  - Free
  - Paid
  - Exchange



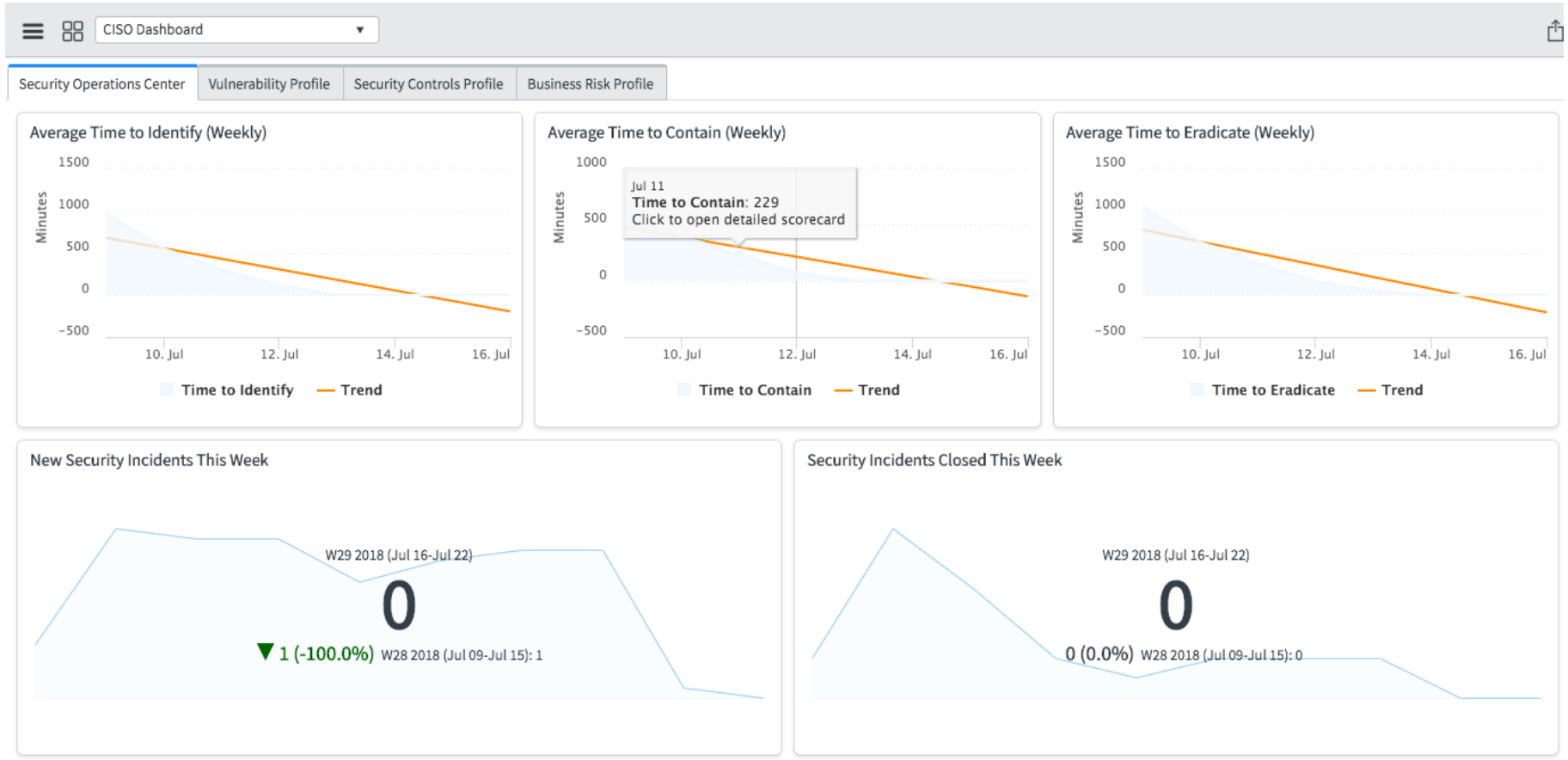
Collaboration

- **Internal to your organization**
  - Infrastructure, Privacy, HR, Marketing, Legal
  - Physical Security, Facilities
- **External**
  - Law enforcement (Infragard)
  - Department of Health and Human Services
  - ISAC (H-ISAC / REN-ISAC)
  - Cyber-Insurance provider
  - Regional groups
  - Old style networking!
- **Two-way!**

Trends

- **Cybersecurity staffing issues**
- **Vendor consolidation and alliances**
- **Social attacks**
- **Ransomware and botnets**
  - IoT as vectors
- **Managed services / Cyber vSOC**
- **Security Orchestration, Automation and Response (SOAR)**
- **Endpoint Detection and Response (EDR)**
- **Cloud Workloads**

Metrics



Servicenow CISO Dashboard

THANK YOU!

QUESTIONS?